GP/2681

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Docket No. **8579.00**

CLAIM FOR BENEFIT OF EARLIER-FILED FOREIGN APPLICATION

Application of

James B. Baird

Serial No. **09/815,373**

Filed: **March 22, 2001**

FOR: **ELECTRONIC WALLET**

Confirmation No.: **4250**

Group Art Unit: **2681**

Examiner: **Unknown**

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231 on AUG 16 2001 (Date of Deposit).

Shirley Doll

Assistant Commissioner for Patents

Washington, D.C. 20231

Sir:

Applicants wish to claim the benefit of the filing date of the earlier G.B. Application Serial No. **0007360.1**, filed on **March 28, 2000**, recited in the Declaration under the provision of 35 U.S.C. 119, and accordingly, Applicants submit herewith a certified copy of said application.

Respectfully submitted,

Michael Chan

Michael Chan
Reg. No. 33,663
Attorney for Applicant(s)

NCR Corporation, Law Department, WHQ5E
1700 S. Patterson Blvd., Dayton, OH 45479-0001
Tel. No. 937-445-4956/Fax No. 937-445-3733

PATENTS • DESIGNS • COPYRIGHT • TRADE MARKS
The Patent Office

INVESTOR IN PEOPLE

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

Signed

Dated 03 JUL 2001

Patents Form 1/77

1/77

The Patent Office

Patents Act 1977
(Rule 16)

Statement of inventorship and of right to grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

The Patent Office

Cardiff Road
Newport
Gwent NP9 1RH

1. Your reference

8579

28MAR00 E524810-1 D02073
P01/7700 0.00-0007360.1

2. Patent application number
(The Patent Office will fill in this part)

0007360.1

28 MAR 2000

3. Full name, address and postcode of the or of each applicant (*underline all surnames*)

NCR INTERNATIONAL, INC
1700 SOUTH PATTERSON BOULEVARD
DAYTON, OHIO 45479
UNITED STATES OF AMERICA

Patents ADP number (*if you know it*) 74093520001

If the applicant is a corporate body, give the country/state of its incorporation

INCORPORATED IN THE STATE OF DELAWARE

4. Title of the invention

ELECTRONIC WALLET

5. Name of your agent (*if you have one*)
"Address for service" in the United Kingdom to which all correspondence should be sent (including the postcode)

B WILLIAMSON
INTERNATIONAL IP DEPARTMENT
NCR LIMITED
206 MARYLEBONE ROAD
LONDON NW1 6LY

Patents ADP number (*if you know it*) 77911767001

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and (*if you know it*) the or each application number

Country	Priority application number (*if you know it*)	Date of Filing (*day/month/year*)

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application	Date of filing (*day/month/year*)

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? (*Answer 'Yes' if:*

a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.
See note (d))

YES

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document.

Continuation sheets of this form

Description	13
Claim(s)	2
Abstract	1
Drawing(s)	2 + 2

10. If you are also filing any of the following, state how many against each item.

Priority documents	
Translation of priority documents	
Statement of inventorship and right to grant of a patent (*Patents Form 7/77*)	
Request for preliminary examination (*Patents Form 9/77*)	1
Request for substantive examination (*Patents Form 10/77*)	
Any other documents (*please specify*)	

11. I/We request the grant of a patent on the basis of this application.

Signature Brian Dibble Date 23/03/2000

12. Name and daytime telephone number of person to contact in the United Kingdom

CHRISTINE SHEPPARD
0171 725 8379

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

a) *If you need help to fill in this form or you have any questions, please contact the Patent Office on 01645 500505*

b) *Write your answers in capital letters using black ink or you may type them.*

c) *If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.*

d) *If you have answered 'Yes' Patents Form 7/77 will need to be filed.*

e) *Once you have filled in the form you must remember to sign and date it.*

f) *For details of the fee and ways to pay please contact the Patent Office.*

ELECTRONIC WALLET

The present invention relates to an electronic currency storage and manipulation device to be carried on the person of a user. The invention further relates to a method of storing electronic currency securely.

The area of "electronic currency" has grown substantially in recent years. While electronic transfers of currency between organisations and banking bodies is commonly used where traceability is not an issue, electronic currency has the advantage that, like cash, the parties are not identifiable in the transaction.

Several means of generating and using electronic currency exist; typically a unique number is generated to serve as a individual "coin", representing a particular monetary value (for example, 1 euro). This number is then "certified" by the currency issuer as being worth 1 euro.

When a user wishes to spend some of their currency, the number is passed to a merchant, who verifies each "coin" with the issuing party, which records each "coin" as it is used, to ensure that each "coin" may only be used once. The issuer reimburses the merchant to the value of the coins, having previously deducted the same value from the user's account.

In order that electronic currency may be readily accessed for purchases without a need to generate coins at every transaction, it is often desirable for an individual to store previously-created coins.

One portable storage device currently used is a "smart card", typically in the form of a plastics card with a memory device mounted thereon, the memory device being used to record data representing a selection of electronic coins. When the user desires to make a transaction, the card is inserted into an appropriate reader, and the necessary data transfers carried out.

However, smart card technology suffers from a number of disadvantages, which have hindered its adoption for certain transactions. One problem is that electronic currency, like cash, does not require authorisation for its use. For example, if a smart card is stolen, the thief may use the certified currency values as if they were their own. Further, like cash, if the card is lost the electronic currency is lost also. An additional problem is the expense of providing users and merchants with the necessary smart cards and reader technology; this has slowed the take-up of this new technology.

It is among the objects of embodiments of the present invention to obviate or alleviate these and other disadvantages of electronic currency systems. This may be achieved, in part, by combining aspects of electronic

currency systems with elements of existing mobile communications technology.

According to a first aspect of the present invention, there is provided a method of making an electronic currency value available to a user, the method comprising the steps of:

verifying the identity of the user, via a portable communications device; and

identifying a currency value available to the user;

said currency value being accessible via said portable communications device.

Thus, embodiments of the present invention enable a user to be identified and to access only that currency which they are authorised to access, by means of a portable communications device, such as a mobile telephone.

Preferably, identification of the currency value requires prior verification of the user's identity.

Alternatively, or in addition, accessing of the currency value requires prior verification of the user's identity.

These steps ensure that use of the currency is reliant upon satisfactory verification of the user's identity. Therefore unauthorised users will be unable to make use of another individual's currency.

Preferably, verification of the user's identity makes use of a biometrics identifier; for example, the

user's iris or fingerprint characteristics, or the user's voice. Methods of biometrics verification will be known to those of skill in the art.

In a preferred embodiment of the method of the present invention, the method further comprises the step of storing said currency value in a storage means provided in said portable communications device. Alternatively, the method may comprise the step of storing said currency value in a storage means accessible via said portable communications device. Preferably, the stored currency value is encrypted by means of an algorithm dependent at least in part on a biometrics characteristic of the user. Therefore, the currency may only be accessed by a user presenting an appropriate biometrics identifier.

According to a second aspect of the present invention, there is provided an apparatus for accessing electronic currency, the apparatus comprising:

means for verifying the identity of a user;

data processing means for responding to user instructions;

means for communicating user instructions to the data processing means; and

a portable communications facility, for sending and receiving data to and from the apparatus.

An apparatus according to the present invention provides a medium for storage and handling of electronic

currency, while being capable of data communication with a remote location, thereby eliminating the need for separate electronic currency smart card readers. The user recognition means may also be used to provide a measure of security to stored currency, such that only an authorised user may access the currency.

Preferably, the user verification means comprises a biometrics recognition device. For example, the device may determine a particular characteristic of a user's fingerprint, iris, or voice, in order to compare the determined characteristic against a reference characteristic. Alternative user verification means may be used, for example, a secret password or numeric code communicated to the data processing means, or the like.

In a preferred embodiment, the apparatus may further comprise data storage means for storing certificated electronic currency values. These currency values may or may not be encrypted, for example with an encryption algorithm derived in part from a particular user's biometric characteristics. In an alternative embodiment, certificated and possibly encrypted electronic currency values are stored remotely, and accessed by means of the portable communications facility. A mixture of these types of storage may also be used, with some currency stored locally, and some remotely.

Preferably the data processing means may include means for encrypting and/or decrypting data. Preferably

also the encryption/decryption means may make use of an algorithm derived in part from a particular user's biometric characteristics. This ensures that each user may use only their own currency: measured biometrics characteristics are used to access a data sequence which has previously been encrypted with the same biometrics characteristics, whether remotely or locally. In this way several different individuals' currency may be stored on the same apparatus, and each user may only access their own currency. Further, the use of this method of encryption/decryption means that it is not necessary for a positive identification of every user to occur, but merely to make available to a user whichever data provides a meaningful output (that is, a currency value) when decrypted with that user's particular characteristics. The task of user recognition is thereby greatly simplified.

Preferably the communications facility may be used for data communication with a mobile telephony network. Preferably the apparatus may function as a mobile communications device. For example, the apparatus may comprise a mobile telephone.

Preferably the apparatus further comprises a local data communications facility. For example, the apparatus may comprise one or more infra-red or other electromagnetic radiation communications ports, or may use low-powered radio signals, or the like. This may be

used in order to communicate data locally (for example, with a merchant's electronic "cash register") without the requirement to be in contact with a remote location (such as a central mobile communications "hub"). For example, the facility may be used to transfer certificated currency values from the data storage means to a second apparatus of this or another aspect of the present invention, or to a merchant's electronic currency "till" or the like. Transactions in electronic currency may thereby be conducted in a relatively rapid and straightforward manner, and do not require the user to be in contact with a remote location (for example, if a mobile telephone signal is weak).

According to a third aspect of the present invention, there is provided a method of securely storing electronic currency values, the method comprising the steps of:

obtaining a biometrics identifier from a user;

generating a request for a certificated currency value;

sending said request to a certified currency issuer;

obtaining a certified currency value from said issuer;

encrypting said certified currency value in a manner dependent at least in part on said biometrics identifier; and

storing the encrypted certified currency value.

This aspect of the present invention provides a method of storing currency values encrypted in such a way that only the owner of the currency may access these values. The encryption itself may be performed locally (for example, by a portable communications device), or remotely (for example, by the currency issuer itself). There is further no necessity to recognise or match the biometrics identifier in order to verify the user, since the encrypted currency will only be accessible to a user presenting the appropriate biometrics identifier to successfully decrypt the currency values. Certain embodiments of the invention may nonetheless incorporate validation of the user's identity in the invention if desired; for example, as an additional layer of security, to ensure that unauthorised individuals may not even access the encrypted currency values.

According to a fifth aspect of the present invention there is provided a method of accessing stored electronic currency, the method comprising the steps of:

obtaining a biometrics identifier from a user;

decrypting an encrypted certificated currency value in a manner dependent at least in part on said biometrics identifier; and

transferring the decrypted certificated currency value to a third party, such as a vendor.

Again, the method of this aspect of the present invention ensures that each user may only access their

own encrypted currency values; if an unauthorised individual attempts to access the currency, the decryption algorithm will not yield a decrypted currency value.

These and other aspects of the present invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

Figure 1 illustrates an apparatus for manipulating electronic currency, in accordance with an embodiment of an aspect of the present invention, in the form of a mobile telephone;

Figure 2 shows a block circuit diagram of components accommodated within the apparatus of Figure 1; and

Figure 3 illustrates a network and the step of transactions involving electronic currency and the apparatus of Figures 1 and 2.

Referring now to Figure 1, there is shown an apparatus 10 for manipulating electronic currency in accordance with one embodiment of an aspect of the present invention, in the form of a mobile telephone. The telephone 10 comprises a plastics outer casing 12 which accommodates a display screen 14 and a numeric keypad 16. Additional multifunction keys 18 are also provided. Further functional items, as will be described, are housed within the casing 12 and are not normally visible to a user.

Figure 2 illustrates schematically the functional components of the apparatus 10. The casing 12 is shown as a dotted line rectangle. A data bus 20 connects a data processor 22, the numeric keypad 16 and multifunction keys 18, a random access memory 24, a portable electronic communications facility 26, a biometrics reader 28, the display screen 14, and an infra-red local communication port 30. The biometrics reader 28 may take the form of a fingerprint reader, an iris scanner, a voice recognition module, or the like.

Figure 3 shows a series of steps involved in typical electronic currency transactions, including a mobile telephone 10, a mobile telephony base station 32, an electronic currency issuer 34, and a merchant 36. Double-headed arrows represent avenues of communication between the component parts of the network.

In order to store electronic currency securely on the telephone 10, the following sequence of events is conducted. Using the numeric keypad 16 and function keys 18, a user selects the appropriate option from a menu displayed by the telephone 10. The biometrics reader 28 then acquires an image of, for example, the user's iris. This is then digitised to provide a unique biometrics identifier. The communications facility 26 is then used to pass a request for currency via a telecommunications base station 32 to an electronic currency issuer 34 with which the user has an account. If desired, the biometrics

identifier may be used to verify the identity of the user by comparing the sampled identifier with a reference identifier for authorised users, either locally by the mobile telephone 10, or remotely, by the currency issuer 34.

The issuer 34 generates certificated currency values to the desired amount, and transmits these back to the telephone 10 via the base station 32. The unencrypted values are then encrypted locally by the data processor 22 using an algorithm derived at least in part from the user's biometrics identifier. Receipt of the currency is acknowledged by the telephone 10, and the encrypted values are then stored in the telephone's RAM 24, until needed. In the case of a mobile telephone, the RAM 24 may form a part of the telephone's SIM.

Alternatively, the encryption may take place remotely, by the currency issuer 34. In this case, the biometrics identifier is passed to the issuer 34 together with a request for currency; and an encrypted certified currency value is returned to the telephone 10.

The encrypted values are also stored with an unencrypted token indicating the value and/or owner of the currency. Either of these methods may also incorporate an additional security measure if desired, by comparing the user's biometrics identifier against a stored reference identifier for that user in order to verify the user's identity. Only verified users would be

permitted to make use of the currency storage and manipulation facilities of the telephone. This comparison may take place either locally, in the telephone 10, or remotely, at the currency issuer 34.

Once the encrypted currency values have been stored in the RAM 24 of the telephone 10, the user may wish to purchase goods or services from a merchant 36.

In order to access the currency, the user enters the appropriate details of the desired currency transaction by means of the numeric and function keypads 16, 18 and the screen 14. The data processor 22 then retrieves suitable encrypted 'coins' to the desired total value from the telephone's RAM 24. A biometric measurement is taken of the user by the biometrics reader 28 (for example, an iris scan), and an identifying value is passed to the data processor 22. This value is then used as the basis for a decryption algorithm to operate on the encrypted currency values, yielding unencrypted certified currency values. If an unauthorised user attempts to access the currency, their biometrics will not yield unencrypted currency values, but rather meaningless data. Thus only the currency owner may have access to their currency.

The encrypted currency values are then passed to the merchant's electronic 'cash register' 36, either directly by means of the short range infra-red communications port

or the like, or indirectly via communications facility 26 and a mobile telephony base station 32.

The merchant 36 may verify the currency with the issuer 34 again either by a direct dedicated network link or via a more general communications network, and may possibly issue "change" to the user, in the form of new certificated currency values.

As an alternative to, or in addition to, the methods described above, the RAM 24 may be situated remotely from the telephone 10, for example with the currency issuer 34. In this case the encrypted currency values are stored remotely, and access to the issuer 34 is required for every transaction. The decryption process will be somewhat modified in this embodiment also, as the biometrics identifier will be passed to the issuer 34 for decryption as well as encryption.

It can be seen from the foregoing that the present invention provides a robust and straightforward means of conducting electronic currency transfers and transactions, and of storing currency values, in such a way that only the currency owner may have access to their money. Further, the provision of the storage and access means in the form of a mobile telecommunications device takes advantage of an already widespread technology. The invention also removes the requirement for users and merchants to acquire specialised smart card readers and the like.

Claims

1. A method of making an electronic currency value available to a user, the method comprising the steps of: verifying the identity of the user, via a portable communications device; and identifying a currency value available to the user; said currency value being accessible via said portable communications device.

2. A method according to claim 1, wherein the step of identifying a currency value requires prior verification of the user's identity.

3. A method according to claim 1 or 2, wherein the method further comprises the step of storing said currency value in a storage means provided in said portable communications device.

4. Apparatus for accessing electronic currency, the apparatus comprising: means for verifying the identity of a user; data processing means for responding to user instructions; means for communicating user instructions to the data processing means; and a portable communications facility for sending and receiving data to and from the apparatus.

5. Apparatus according to claim 4, wherein the user verification means comprises a biometrics recognition device.

6. Apparatus according to claim 4 or 5, wherein the apparatus further comprises data storage means for storing certificated electronic currency values.

7. Apparatus according to any of claims 4 to 6, wherein the data processing means may include means for encrypting and/or decrypting data.

8. Apparatus according to any of claims 4 to 7, wherein the communications facility is used for data communication with a mobile telephony network.

9. Apparatus according to any of claims 4 to 8, wherein the apparatus functions as a mobile communications device.

10. Apparatus according to any of claims 4 to 9, wherein the apparatus further comprises a local data communications facility.

11. A method of securely storing electronic currency values, the method comprising the steps of: obtaining a biometrics identifier from a user; generating a request for a certificated currency value; sending said request to a certified currency issuer; obtaining a certified currency value from said issuer; encrypting said certified currency value in a manner dependent at least in part on said biometrics identifier; and storing the encrypted certified currency value.

ELECTRONIC WALLET

Abstract

A method of making an electronic currency value available to a user is described. The method comprises the steps of: verifying the identity of the user, via a portable communications device; and identifying a currency value available to the user; said currency value being accessible via said portable communications device. Apparatus for accessing electronic currency is also described. The apparatus comprises: means for verifying the identity of a user; data processing means for responding to user instructions; means for communicating user instructions to the data processing means; and a portable communications facility for sending and receiving data to and from the apparatus.

[Fig 2]

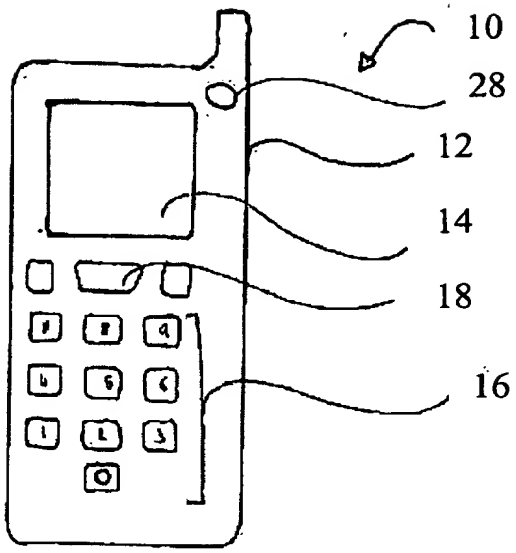
10
28
12
14
18
16

Fig 1

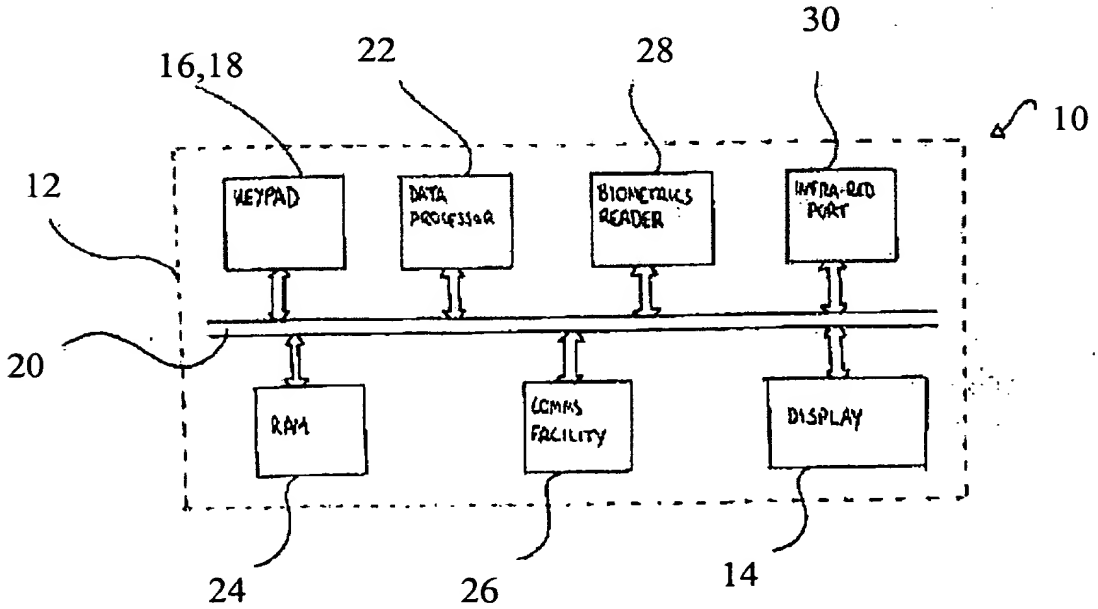
16,18
22
28
30
10
12
KEYPAD
DATA PROCESSOR
BIOMETRICS READER
INFRA-RED PORT
20
RAM
COMMS FACILITY
DISPLAY
24
26
14

Fig 2

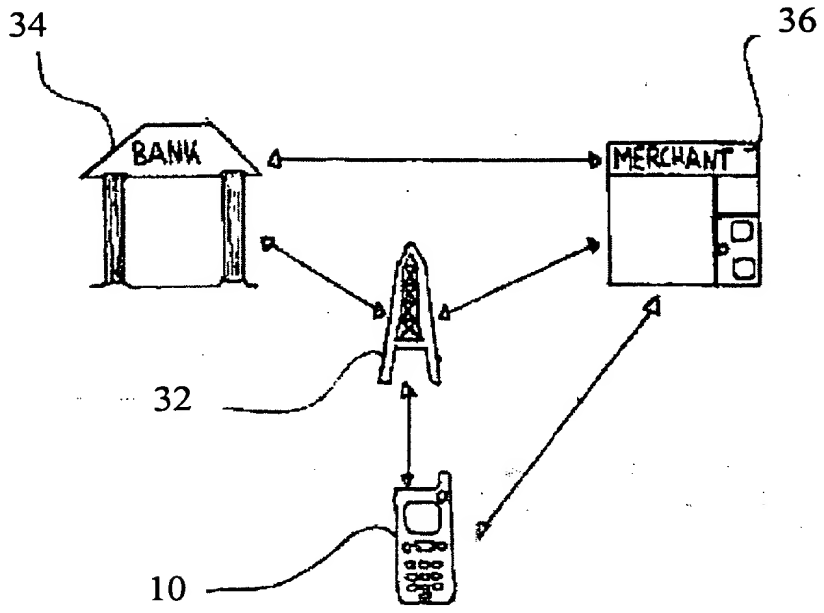

Fig 3